From: Kerman, Sara J. (Fed)
To: Moody, Dustin (Fed)
Subject: RE: new FAQ question for our PQC page
Date: Thursday, July 20, 2017 11:27:00 AM

Done.

From: Moody, Dustin (Fed)
Sent: Wednesday, July 19, 2017 3:20 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: new FAQ question for our PQC page

Sara,

Can you post this to our FAQ page sometime? Thanks,

Dustin

Q: How should submitters choose symmetric algorithms for their submissions?

A: While NIST will permit submitters to choose any NIST approved cryptographic algorithm for their submission if they feel it is necessary to achieve the desired security and performance, a number of potential submitters have asked us to offer default options for common symmetric cryptographic primitives. As such, here are our suggestions:

1) Hash functions: SHA512 is likely sufficient to meet the requirements of any of our five security strength categories and gives good performance in software, especially for 64 bit architectures. Submitters seeking a variable length output, good performance in hardware, or multiple input strings, may instead prefer to use TupleHash256 (specified in SP 800-185.)
2) XOFs: We would recommend SHAKE256
3) Authenticated encryption: We'd suggest AES256-GCM with a random IV.
4) PRFs: Where security proofs can accommodate something that is not indifferentiable from a random oracle, John's AES-based seed-expander will offer excellent performance. Otherwise, KMAC256 (specified in SP 800-185) will be a good choice.

Also recall, from the CFP: "If the scheme uses a cryptographic primitive that has not been approved by NIST, the submitter shall provide an explanation for why a NIST-approved primitive would not be suitable."